Abstract

This invention concerns a consumable authentication protocol for validating the existence of an untrusted authentication chip, as well as ensuring that the Authentication Chip lasts only as long as the consumable. In a further aspect it concerns a consumable authentication system for the protocol. In this invention we are concerned not only with validating that an authentication chip is present, but writes and reads of the authentication chip's memory space must be authenticated as well. A random number is encrypted using a first key and sent to an untrusted chip. In the untrusted chip it is decrypted using a secret key and re-encrytped together with a data message read from the untrusted chip. This is decrypted so that a comparison can be with the generated random number and the read data message.